Transaction Network Services

One Connection – A World of Opportunities

# 2019 Robocall Investigation Report

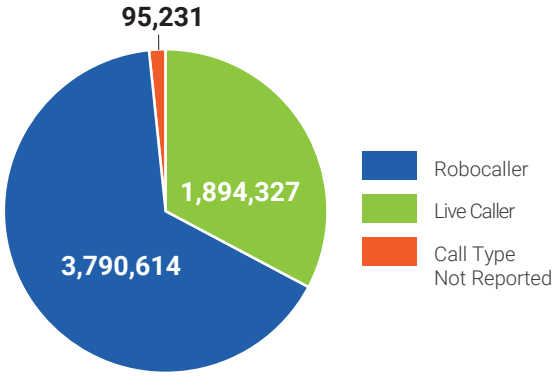
Author: Transaction Network Services

Date: March 2019

## Table of Contents

# Executive Summary

Robocalling, spamming, scamming, spoofing are scenarios that play out for consumers multiple times a week - if not every day. The FTC has received 3.7 million complaints for FY 2018, surprisingly down from 4.5 million complaints in FY 2017, but still the number one consumer complaint. The top complaints were about robocalls professing to reduce debt[1].




The FCC has focused significant policy-making and enforcement resources on confronting malicious caller ID spoofing. Changes in technology have made it easier and cheaper for scammers to make robocalls and to manipulate caller ID information.

The agency fined telemarketer Mr. Philip Roesel and his companies more than $82 million for illegal caller ID spoofing and imposed more than $37.5 million fine against Affordable Enterprises of Arizona for purportedly making millions of illegally-spoofed telemarketing calls that appeared to originate from consumers and other numbers not assigned to the company.

In addition, a $120 million fine was levied against Mr. Adrian Abramovich for similar activity.[2] In November of 2017, the FCC adopted rules allowing providers to block calls from phone numbers on a Do-Not-Originate (DNO) list and those that purport to be from invalid, unallocated, or unused numbers.

Carriers have begun to block some of these calls permissible by the FCC order. Carriers also have made low-cost tools available to their wireless subscribers, and have educated them on robocalling.

The efforts between enforcement, carrier activity and subscriber knowledge of robocalling activity and perhaps consumer fatigue has led to a reduced number of complaints received by the FTC.

The problem is not unique to the United States. In the past year more than 740,000 Canadians have complained to the Canadian Anti-Fraud Centre about being targeted by a phone scam, according to Ian Ross, Chairman & CEO of Canadian Radio-television Telecommunications Commission (CRTC), at a recent SIPNOC Forum presentation.

*Complaints to the FTC have dropped for the first year ever*

[1] https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/national-do-not-call-registry-data-book-fy-10
[2] https://www.fcc.gov/document/fcc-fines-robocaller-82-million-illegally-spoofed-calls, https://www.fcc.gov/document/fcc-proposes-375-million-fine-spoofed-telemarketing-calls, https://www.fcc.gov/document/fcc-fines-massive-neighbor-spoofing-robocall-operation-120-million

The 2019 Robocall Investigation Report is an update to the trends found in the 2018 Robocall Investigation Report. TNS Call Guardian, the industry-leading big-data analytics engine, has gained insights and reputation on over 1.5 billion phone numbers by analyzing a billion daily call events across hundreds of carriers.

In addition, this report leverages consumer feedback provided by users of carrier deployed Enhanced Caller ID services powered by TNS, deployed to over 200M mobile devices across more than 500 makes and models.

Billions of data points weave together the robocall stories and statistics from across the country. What valuable insights can your organization learn from them?

Here is a sample of findings discussed in this report:

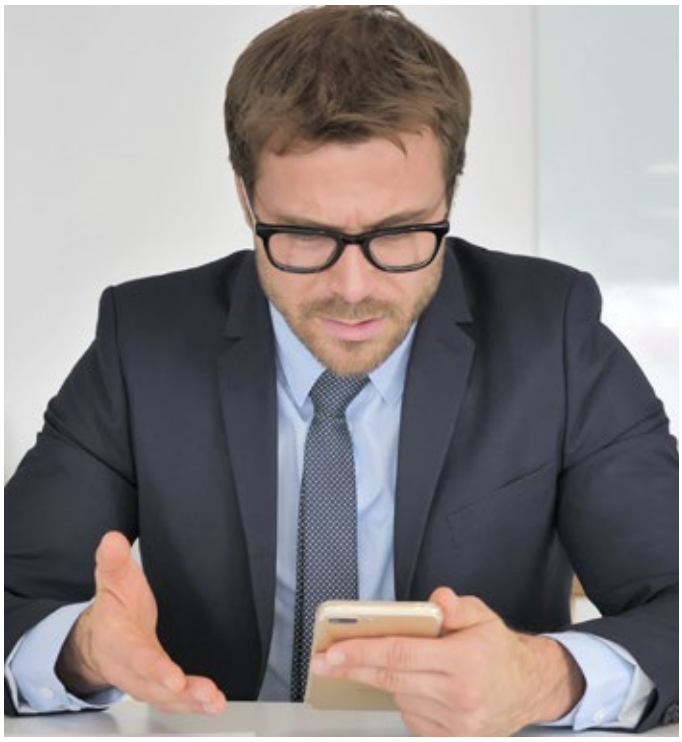
- **Robocall spoofers hijacking mobile numbers.** 1 in 4,000 mobile numbers are now being hijacked by robocall spoofers every month, which is causing 20% of people who have had their number hijacked to disconnect their phone.
- **Neighbor spoofing & snowshoe spamming more sophisticated.** High risk (scam/fraud) calls using neighbor spoofing now accounts for 24% of all negative calls - up 5 percentage points from the prior year. Spoofers are also more elusive, using snowshoe spamming to propagate spoofing over several telephone numbers in low volume and rapidly churning through them to evade detection.
- **Legitimate customer care numbers are being spoofed.** More than two-thirds of the calls from legitimate toll-free numbers are identified as nuisance or high-risk.
- **Tier 1 carriers aren't the problem.** Almost three-quarters of all calls, positive and negative, come from tier one providers, yet a little over 10% of the calls from those carriers are considered high-risk.
- **Negative traffic from Canada is growing at over 100%.** Originating Canadian inter-carrier calls labeled as nuisance and high-risk saw an increase of over 100% from first to fourth quarter.

# Introduction

The 2019 Robocall Investigation Report by TNS includes a vast amount of factual evidence derived from real network traffic over the last three years. The study is unique in that it offers an objective, first-hand view of robocalling, spamming and spoofing across the hundreds of carriers that signal across the TNS signaling and database routing infrastructure.

Since 1990, TNS has managed some of the largest real-time data communication networks in the world, enabling industry participants to simply, securely and reliably interact and transact with other businesses, to access the data and applications they need, over managed and secure communications platforms. TNS leads the development of solutions to help carriers navigate a host of infrastructure complexities and maximize their network reach through the creation of unique multi-service hub solutions.

In this report, we have attempted to interpret the robocall trends and hope that your organization and consumers will learn from these findings.



# Primer on Robocalling

The Telephone Consumer Protection Act or TCPA was passed by Congress in 1991 to regulate the use of automatic telephone dialing systems ("auto-dialers") and prerecorded voice messages. The specifics of the regulation and the courts' interpretation are complex and sometimes difficult to decipher but the essence of the law is to safeguard consumer privacy by mandating robocallers obtain explicit consent before placing any 'non-emergency' robocall to a consumer's cell phone, or to mobile and landline phones that have been registered on the Do Not Call list.

A robocall is a phone call that uses a computerized auto-dialer to deliver a pre-recorded message, as if from a robot. Robocalls are often associated with political and telemarketing phone campaigns but can also be used for public-service or emergency announcements. Some robocalls use personalized audio messages to simulate an actual personal phone call[3].

## *Fraud from unwanted calls amounts to about $9.5 billion annually*

When the call is answered, the auto-dialer either connects the call to a live person or plays a pre-recorded message. Both are considered robocalls.

Robocalls are popular with many verticals, such as real estate, healthcare, telemarketing and direct sales companies. Many companies who use robocalling are legitimate businesses, but some are not. Those illegitimate businesses may not just be annoying consumers, they also may be trying to defraud them. Fraud from unwanted calls amounts to about $9.5 billion annually, according to the FTC. Not everyone files a complaint, "so you can extrapolate significantly upwards from that to get a sense of this problem," according to Brendan Carr, FCC Commissioner[4].

Fraud has become easier for criminals as technology, such as VoIP calling, has enabled both spoofing of a number and low cost robo-dialing, and Americans are more likely to answer unknown calls on their mobile phones.

Many robocalls are not wanted and several methods have been developed to prevent unwanted robocalls. The United States has developed the Do-Not-Call Registry which was created in 2003 and allows consumers to "opt out" of receiving telemarketing calls on their landline and mobile phones, regardless of whether they are robocalls or not. As of September 30, 2018, the registry had over 235 million active registrations,[4] up from about 230 million[5] at the same time in 2017.

However, the lists have been ineffective. While legitimate call originators honor the list, illegitimate callers ignore it. Consequently, a market has developed for products that allow consumers to block robocalls. Most products use methods like those used to mitigate SPIT (spam over Internet telephony) and can be broadly categorized by the primary method used. However, due to the complexity of the problem, no single method is sufficiently reliable[6].

[3] https://en.wikipedia.org/wiki/Robocall
[4]https://www.usatoday.com/story/tech/news/2018/03/23/robocall-battle-continues-fcc-and-ftc/453782002/
[5] https://www.ftc.gov/news-events/press-releases/2018/12/ftc-releases-fy-2018-national-do-not-call-registry-data-book-mini
[6] https://ieeexplore.ieee.org/document/7546510/

# Methodology

By creating an industry-leading big data analytics engine, TNS Call Guardian, TNS has maintained a strong focus on aiding calling provider partners as they seek to restore trust in voice calls. TNS' Call Guardian product analyzes over one billion call events across hundreds of carriers every day and bases robocall scoring and categorization on this data.

TNS ensures that Call Guardian evolves in response to emerging bad actor trends, such as neighbor spoofing and perceives the evolution of bad actor calling tactics as a response to the success the industry is seeing in addressing current bad actor methodologies. Neighbor spoofing occurs when the information on the receiver's phone matches or closely matches the area code and digits similar to one's own phone number.

TNS can provide unique intelligence because of the combination of deep network integration into partner carrier networks combined with a layered approach of solutions, including real-time analytics which provides unique visibility beyond honey traps and blacklists. A layered approach allows TNS to create accurate and comprehensive reputation profiles differentiating legitimate users of telecommunications services from abusive, fraudulent, and unlawful users.

A honey trap or honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked[7].

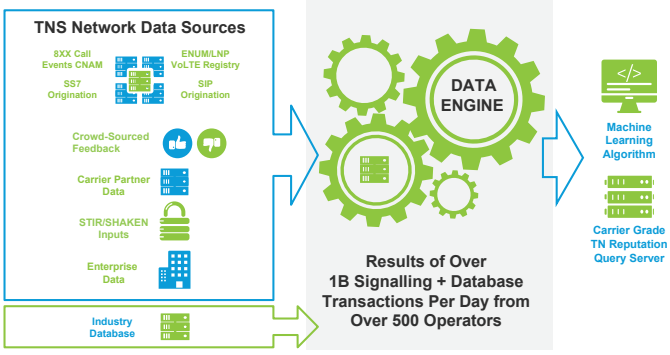
The underlying TNS Call Guardian service architecture is akin to dynamic reputation systems, not to be confused with static list-based reputation systems that contain information of known or previously encountered threats and are typically distributed in the form of blacklists or whitelists. Rather, the service functions similar to a trusted credit reporting service continuously collecting reputation data from multiple sources, relying on a mix of historical reputation data and "real-time" intelligence – making use of known legitimate and malicious behavior to train a machine learning algorithm in order to project reputations on virtually any telephone number ("TN") for which there is little or no available crowd-sourced reputation data.

Call management and caller identification applications designed to protect legitimate users of telecommunications services ("end-users") from illegal robocalls and phone calling scams, form a major application area for the service.

These applications are an important source of crowd-sourced reputation data and rely on the service to provide insight that helps identify callers who may be violating state and federal laws governing the use of automatic telephone dialing systems ("auto-dialers") and caller ID spoofing technologies, most notably scammers who unlawfully use telecommunications services in the commission of a crime of identity theft or fraud and spammers who in willful non-compliance of TCPA, place automated calls, both telemarketing and informational, without the caller's prior consent.

The dynamic nature of the service means that non-binary reputation "scores" along with other helpful insights are supplied on a query-answer basis. Instead of lists, the service supports queries to APIs to ensure the most accurate reputation score is made available in real-time.

TNS provides Enhanced Caller ID that is used by the majority of leading U.S. wireless service providers as well as Call Guardian robocall mitigation services to U.S. landline providers.




[7] https://en.wikipedia.org/wiki/Honeypot_(computing)

# Results and Analysis

## Reputation Category and Scoring

TNS uses reputation categories as a label assigned to telephone numbers observed to have common call behavior. Reputation score provides insight as to the certainty of this categorization and severity of consequences, if any, should an associated threat eventuate.

Categories are indicative of legitimate, abusive, fraudulent and unlawful call behavior - inclusive of any call placed with an auto-dialer or manually dialed. Each carrier can choose what category to display on the device, for example “Potential Spam”. TNS offers a dispute resolution process for call originators to dispute reputational categories assigned to its telephone numbers.

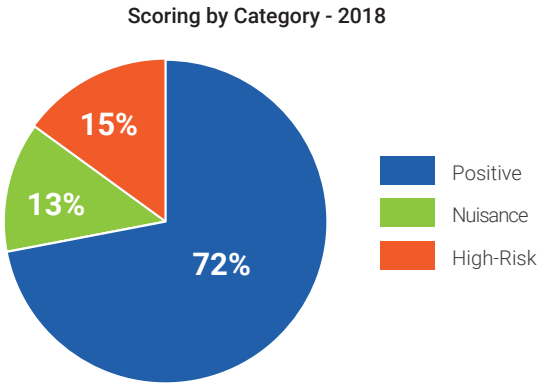

## Scoring of Calls

Reputation scores provide qualitative information about categorization certainty and severity of consequences should an associated threat, if any, eventuate.

The severity of harm of a call considered to be a nuisance call is moderate. The calling behavior of a nuisance call isn’t indicative of malicious intent or negligent non-compliance, but rather of careless, unintentional calling patterns.

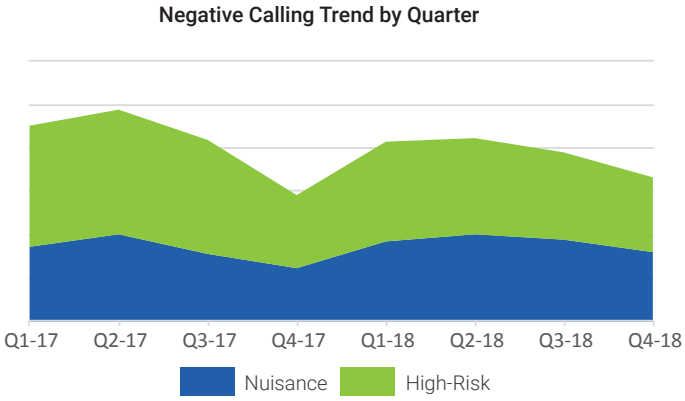
The severity of harm of a high-risk call is deemed major as impact of identity theft can be catastrophic and the associated invasion of privacy can cause severe emotional distress. The resulting loss of money and time and emotional impact is similar to that experienced by a victim of a crime. Typically, deceptive caller ID practices are employed to avoid detection or deceitfully gain caller’s trust.

TNS found that less than 30% the inter-carrier calls were scored negatively, which is an improvement from earlier findings, but consistent with other observations, and summarized below:

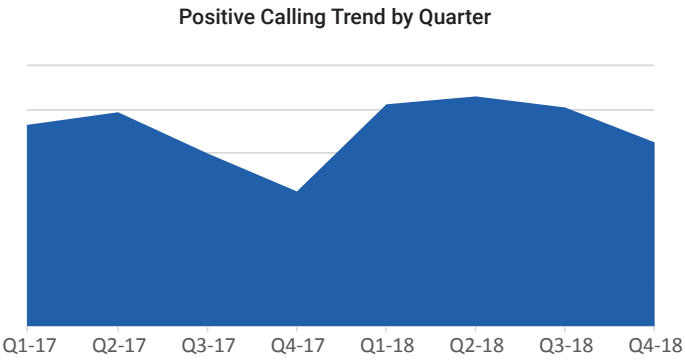



*Nearly 30% of all calls are negative*

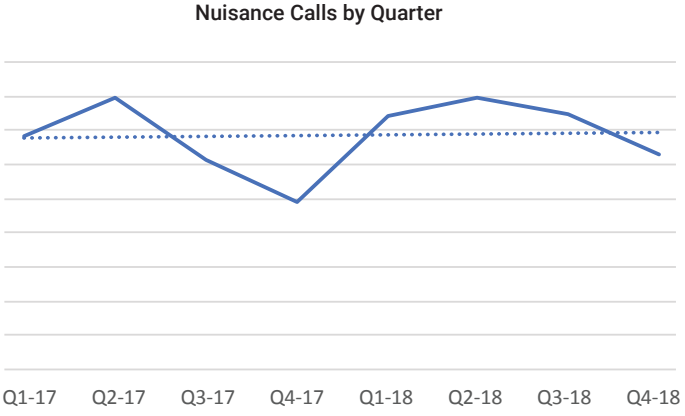
High risk calls (-3, -4) are larger in volume than the nuisance calls (-2), although the high-risk calls are tracking downward with nuisance calls continuing to increase year over year.




The number of positive calls has increased 18% from 2017 to 2018.

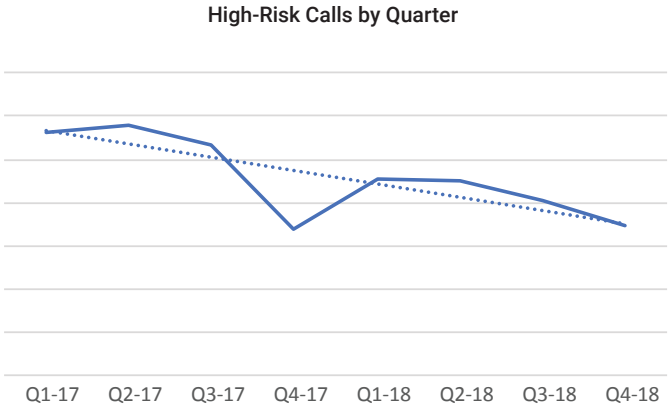



Nuisance calls have increased 13% from 2017 to 2018.




## *Nuisance calls increased by 13% from 2017 to 2018*

While high-risk calls have decreased by 18% from 2017 to 2018.




## *Enforcement by the FCC and carrier action have reduced the number of high-risk calls*

According to a filing with the FCC in January 2019, service providers like AT&T have indicated that since October 2016, they have blocked approximately 4.5 billion illegal calls traversing its wholesale network.

**In addition, recent enforcement actions from the FCC include[8]:**

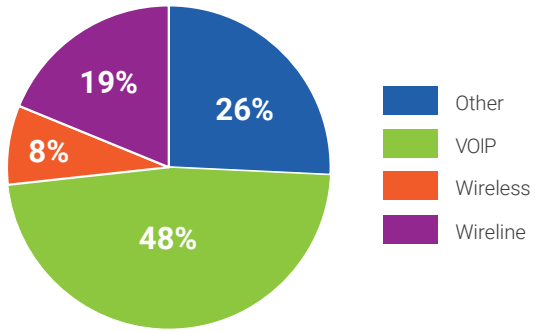
- A record $120 million fine of Florida-based time-share marketing operation that made almost 100 million spoofed calls over three-month period.
- A $82 million fine of a telemarketer which made more than 21 million robocalls to market health insurance.
- A $37.5 million proposed fine of an Arizona marketer which apparently made millions of spoofed calls that appeared to come from consumers.

[8]https://www.fcc.gov/document/fcc-urges-more-phone-industry-join-tracing-scam-robocalls

## Origination of Negatively Scored Calls

Not surprisingly, VoIP-originated calls continue to generate almost 50% of the negatively scored calls by total volume.

**Distribution of all Negatively Scored Calls**




A provider that allows users to bring their own device and unbundles service so that direct inward dial numbers may be purchased separately from outbound calling minutes will be more flexible.

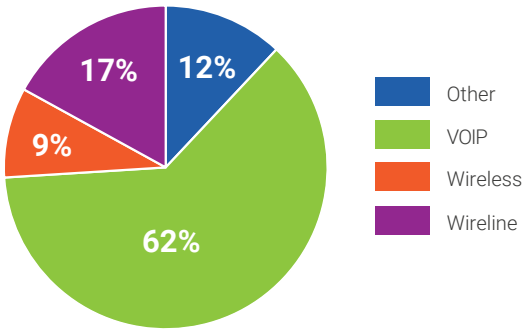
A carrier which doesn't follow established hardware standards (such as Skype) or locks subscribers out of configuration settings on hardware which the subscriber owns outright (such as Vonage) is more restrictive. Providers which market "wholesale VoIP" are typically intended to allow any displayed number to be sent, as resellers will want their customer's numbers to appear[9].

There are legitimate reasons to modify the calling number, however, bad actors use this same technique to hide their identity.

*VoIP originated calls generated over 60% of the high-risk calls by total volume*

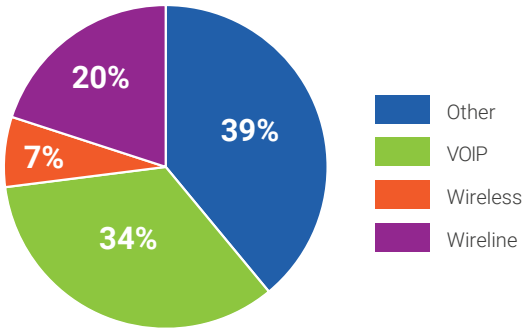
However, looking closer at the data, almost two-thirds of the high-risk calls originate from a VoIP network.

**Distribution of High-Risk Calls**




The distribution of nuisance calls is led by VoIP and other non-carrier assigned numbers.

**Distribution of Nuisance Calls**

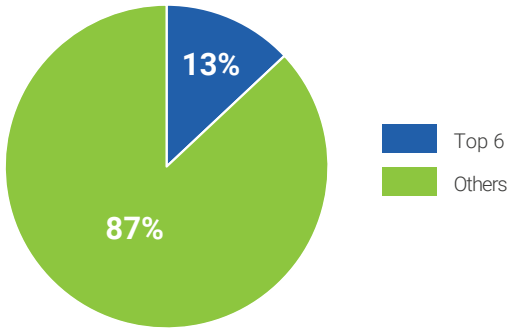



The other category represents toll-free, malformed and invalid telephone numbers. A malformed telephone number is a telephone number that does not have 11 digits or that does not start with 1. An invalid telephone number, unlike a malformed telephone number, is well formed, but is not in a valid LERG block (NPA-NXX) and not in a valid toll-free area code.

Note, only a little over 10% of the high-risk calls are from numbers owned by the top 6 carriers - AT&T, CenturyLink, Comcast, Sprint, T-Mobile and Verizon.

[9]https://www.fcc.gov/document/fcc-urges-more-phone-industry-join-tracing-scam-robocalls

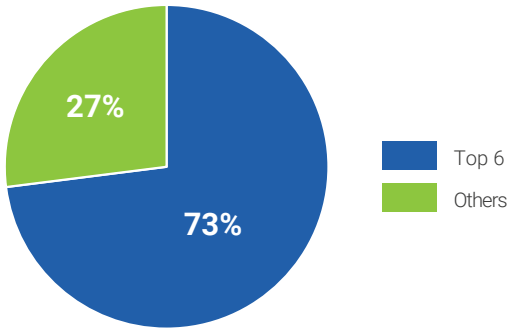
**Network of High-Risk Calls**




However, the top 6 carriers represent almost 75% of total number of calls.

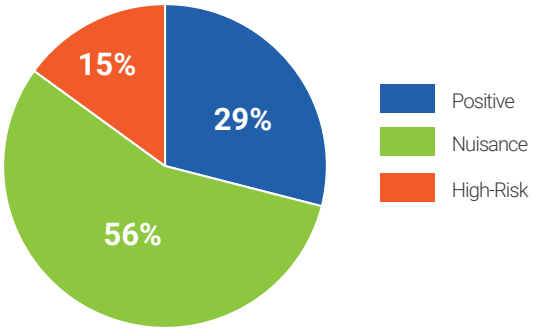
## *Only about over 10% of calls from tier 1 carriers are considered high-risk*

**Network of Total Calls**



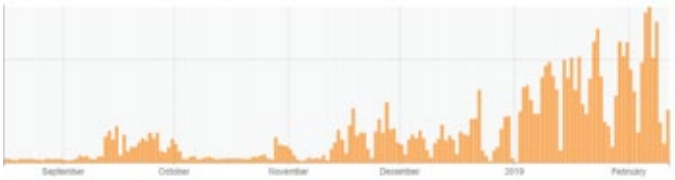

More than two-thirds of the calls from toll-free numbers are considered nuisance or high-risk, much higher than VoIP originated calls.

**Distribution of Calls by Toll-Free Numbers**

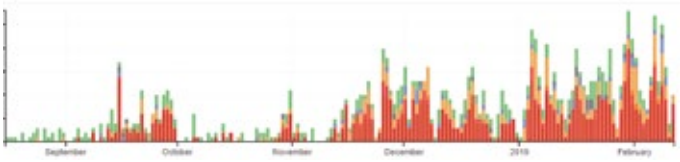



## *Legitimate customer care numbers are being spoofed*

A common technique used by the bad actors is to spoof a legitimate toll-free number which then appears to a subscriber that the number calling them is legitimate. Below is an example of a customer care number of a legitimate enterprise that shows how the number was being spoofed for a period of time.

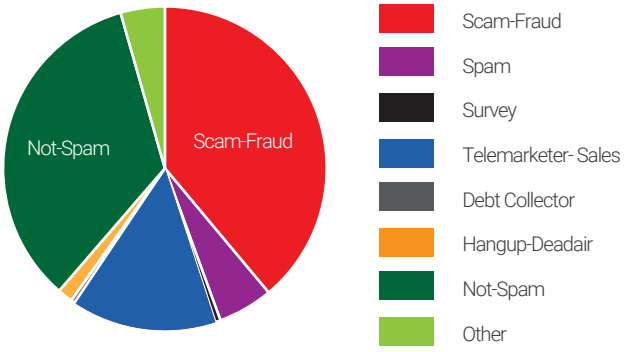


The crowd-sentiment validates that that the legitimate toll-free number is being spoofed.



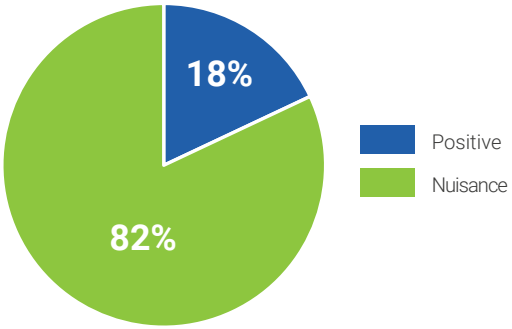
User generated feedback shows that the toll-free number is being used for legitimate purposes but is also being spoofed as part of scam campaign. The color of feedback corresponds to the color in the pie chart below, with dark red being reports of scam-fraud.

**Category Distribution**




The top 10 toll-free numbers, in terms of volume, are overwhelmingly considered nuisance calls by consumers.

**Top 10 Toll-Free Numbers by Volume**




Specific to enterprises, one commonly observed trend is enterprises whose main toll-free number is used for multiple purposes tend to get flagged by analytics engines and receive very mixed feedback from consumers. TNS recommends segmenting the use of toll-free numbers for various enterprise purposes.

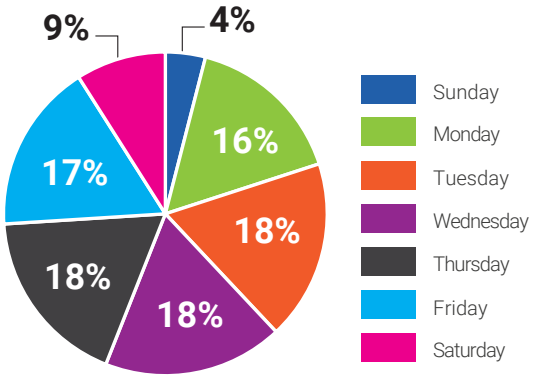
A number used for accounts receivable management, for example, should not be used for other purposes, as consumers will invariably provide negative feedback about the number which will impact other outreach efforts via the same number.

*Over 80% of calls from the top 10 toll-free numbers are nuisance*

## Day of Week

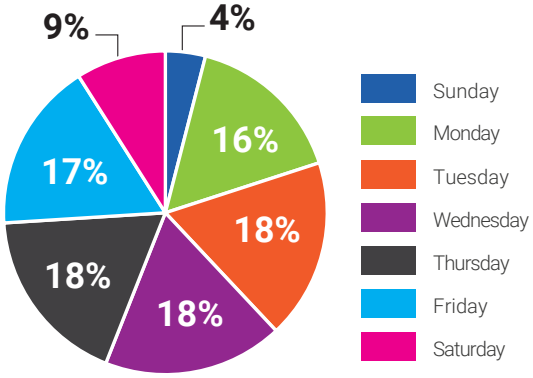
The number of negatively scored calls varies daily with the highest volume on Tuesday, Wednesday and Thursday are the highest days for negative calls at 18%, while the weekend is lower at 13%.

**Day of Week All Negative Calls**



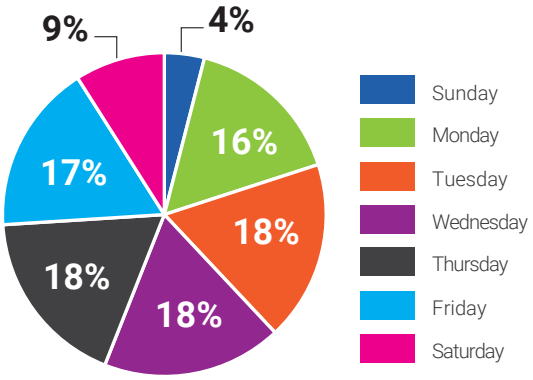

The day of week for nuisance calls and high-risk calls are nearly the same.

**Day of Week for Nuisance Calls**




*Bad actors don't take off the weekends*

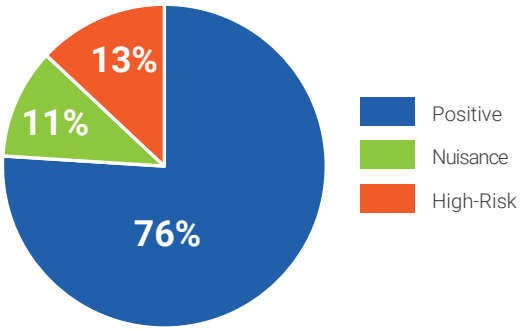
**Day of Week for High-Risk Calls**




Bad actors don't take off the holidays, either, as can be seen by the following charts.

On New Year's Day in 2018, nearly 25% of the calls were negative.

**New Years Day 2018**

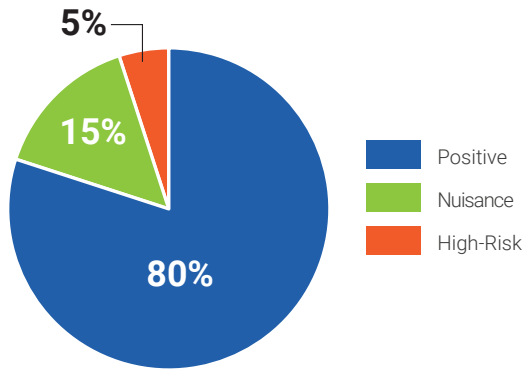



.

New Year's Day wasn't as bad in 2019 to start this year, negative calling dropped by 4%.

## *Bad actors don't take off holidays*

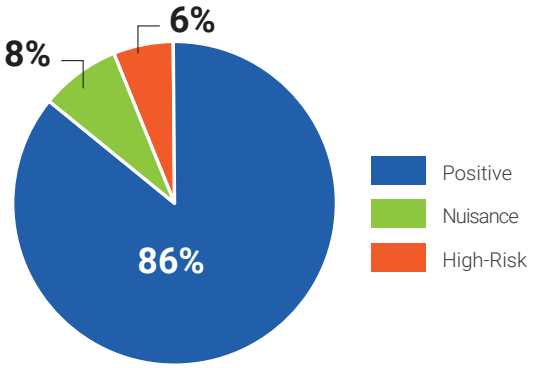
**New Years Day 2019**




The top "scam" on New Year's Day was consistent from 2018 to 2019 with bad actors spoofing as debt collectors to try to gain social security numbers of unsuspecting subscribers.

The bad actors took a little bit of a break for Christmas in 2018 and negative calling was lower than typical and behaved more like a typical weekend day.

**Christmas 2018**

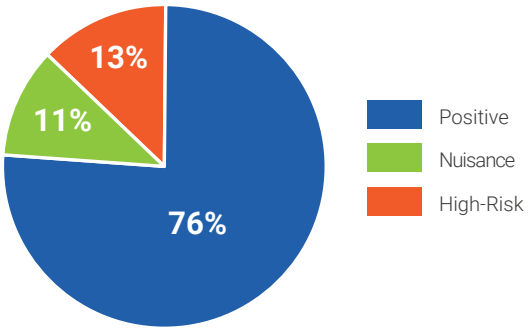



The top "scam" on Christmas this year was from a purported loved one, who is a prison inmate, asking the called party to add money to an account.

Apple's toll-free number appeared to be spoofed, as well, with callers trying to get an unknowing subscriber's personal information.

Thanksgiving was worse than Christmas this year with nearly 25% of the calls generated as negative.

**Thanksgiving 2018**



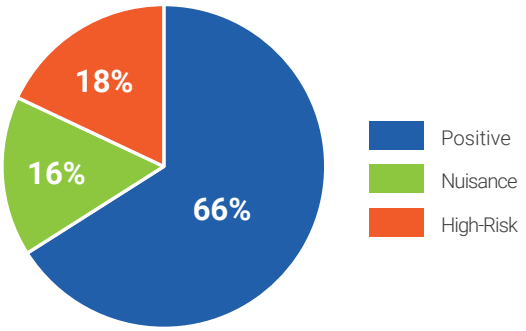

The top "scams" this year were from rewards departments claiming the called party had won a dream vacation. Second on the list was from bad actors claiming that called parties had been given a free cash advance loan and callers were seeking social security numbers, so the subscriber could be given the cash advance.

An invalid number, 555-123-4567, seems to be a favorite with the bad actors and was one of the top negative numbers in volume for Thanksgiving.

# *Tax Day was the highest negative day of the year in 2018*

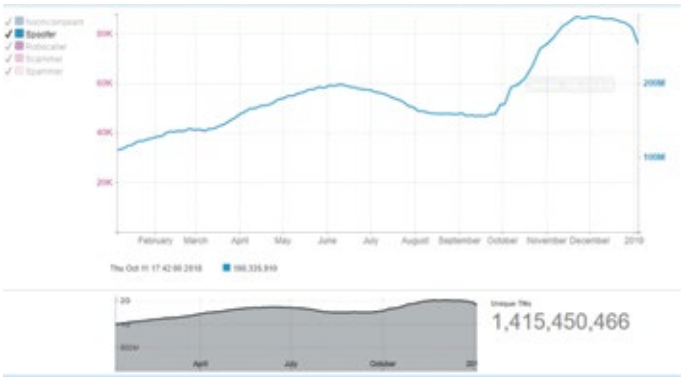
The day with the highest volume of negative calling this past year was on Tax Day, April 17th. Below is the distribution of calls which shows a slightly higher number of high-risk calls than a typical Tuesday.

**Distribution of Calls - April 17th**




## Invalid/Unallocated Number Use

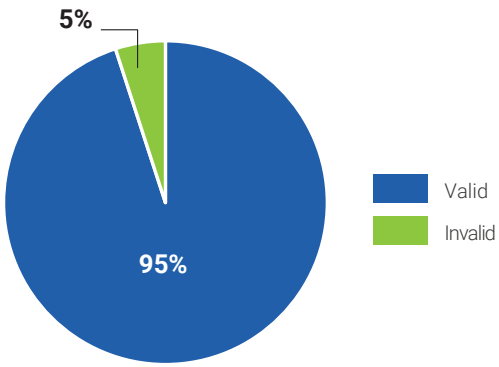
If those whose work has been focused on detecting and addressing nuisance and illegal robocalls know one thing, it is that bad actors change tactics quickly. Use of spoofed numbers is one of those tactics. Spoofing of invalid/unallocated numbers has increased but is still a small percentage of total negative traffic.




The number of unique telephone numbers in the TNS reputation database is larger than the total number of assigned numbers in North America due to 1.) the use of spoofed numbers and 2.) the broader view of inter-carrier call events TNS processes across its signaling and routing infrastructure where these spoofed numbers can be detected. The number of invalid/unallocated spoofed telephone numbers appears to be falling off at certain times, but certain telephone numbers fall off the list due to inactivity.

Only 5% of negative calls are from invalid/unallocated numbers and much of the time such calls can be corroborated as spam calls from our crowd-source information.

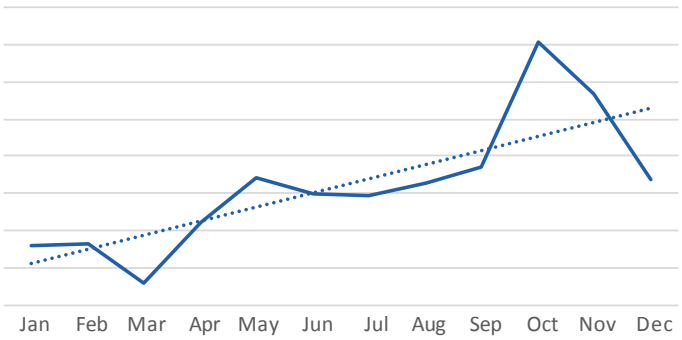
**Negatively Scored Calls by Valid/Invalid NPA-NXX**




*Use of invalid numbers is a small percentage of the problem*

However, the number of negative calls from invalid NPA-NXXs has continued to increase by a factor of 2X.

**Negative Calls Generated by Invalid NPA-NXX**




In November of 2017, the FCC adopted rules allowing providers to block calls from phone numbers on a Do-Not-Originate (DNO) list and those that purport to be from invalid, unallocated, or unused numbers.

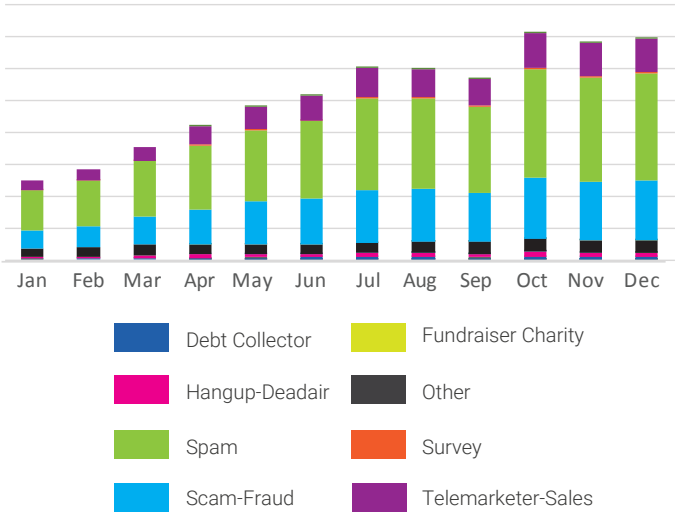
## Crowd-Source Statistics

As part of its Identity and Protection portfolio of services, TNS provides Enhanced Caller ID that is used by the majority of leading U.S. wireless service providers, as well as Call Guardian robocall mitigation services to US landline providers. Enhanced Caller ID identifies callers or texters with their names displayed directly in the incoming call screen and message threads, even if their number is not in contacts.

*Consumers are showing that they want to actively participate and help identify bad actors*

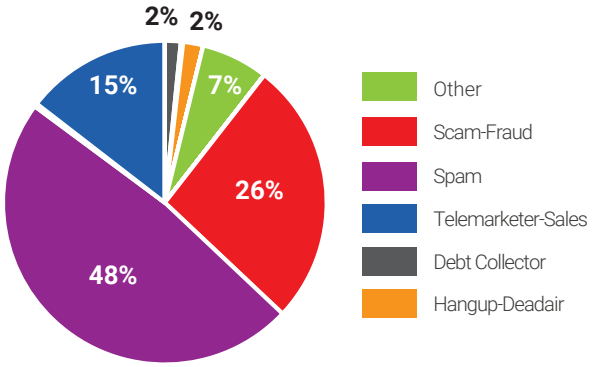
In addition, the amount of crowd-source information TNS has received more than doubled from the first quarter to the fourth quarter of the year. Consumers are showing that they want to actively participate and help identify bad actors.

**Crowd-Source by Volume**




The end-users of the TNS services provide direct feedback through interfaces on the mobile device and they have classified their robocalls in the following categories. Three quarters of the crowd source data is classified as spam or scam-fraud, and 15% is marked as telemarketing sales by end users.

**Crowd-Source Statistics by Category**



## Neighbor Spoofing

TNS launched its Neighbor Spoofing feature mid-year in 2018 that enables carriers to protect their subscribers from the increasingly popular neighbor spoofing robocall tactic.

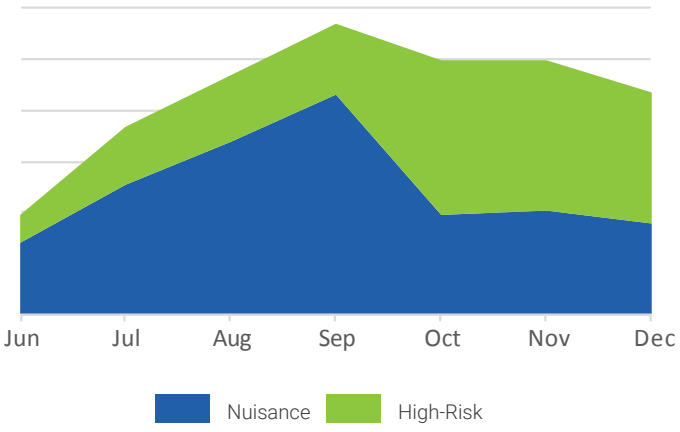
With neighbor spoofing, no matter where the call originates, the information on the receiver's phone matches or closely matches the area code and several digits similar to one's own phone number – which makes the consumer more likely to trust the call and pick up.

TNS' neighbor spoofing feature analyzes, detects and establishes a reputation for phone numbers and phone calls to help consumers evaluate if a phone call with a familiar area code is legitimate.

The combination of deep network integration with carrier partner networks combined with real-time intelligence of the Call Guardian solution is why TNS is leading in combatting this tactic.

TNS has seen an increase of 39% in neighbor spoofing of negative calls from the third quarter to the fourth quarter.

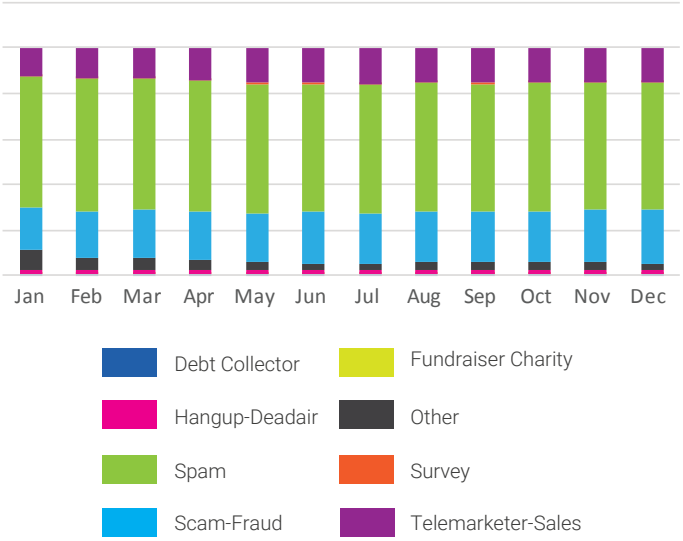
**Neighbor Spoofing - Negative Call Guardian Events**



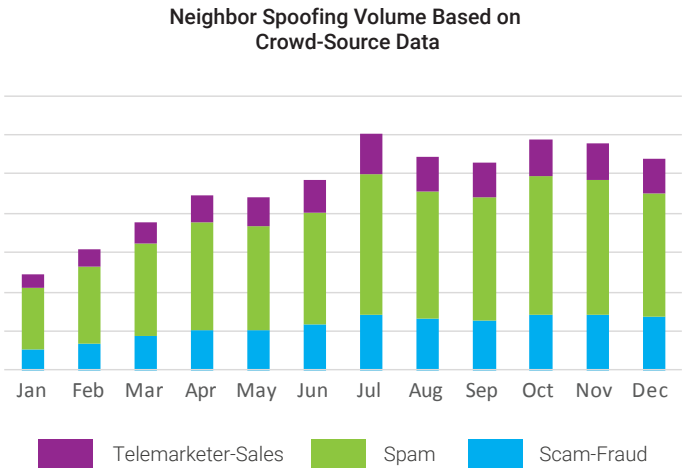

When analyzing the calls where the calling number and the called number are similar, using crowd-source information, the percent of scam-fraud has increased from 19% of the events to 24% of events reported over the year.

*Use of neighbor spoofing increased 39% from 3Q to 4Q*

**Neighbor Spoofing Based on Crowd-Source Data**



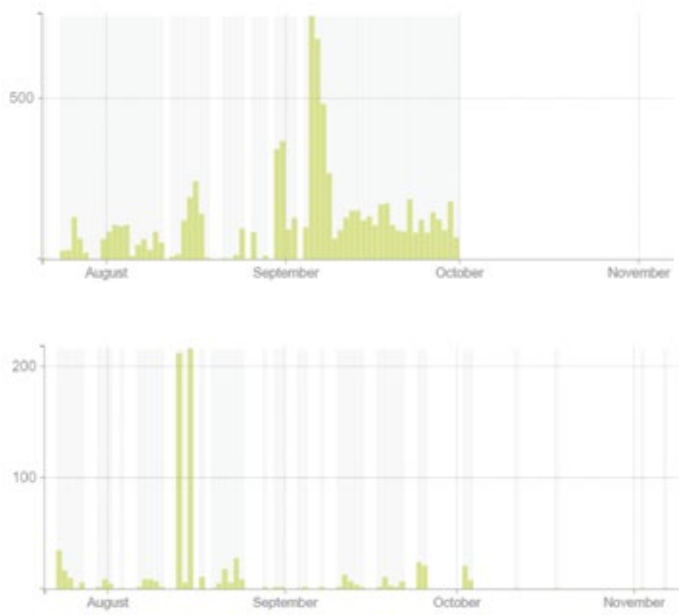
In addition, the crowd-sourced data shows the amount of neighbor spoofing from categories labeled as scam-fraud, spam and telemarketing has increased by 80% from the first quarter to the fourth quarter of this year.




## *Crowd-source feedback shows neighbor spoofing increased 80% from 1Q to 4Q*

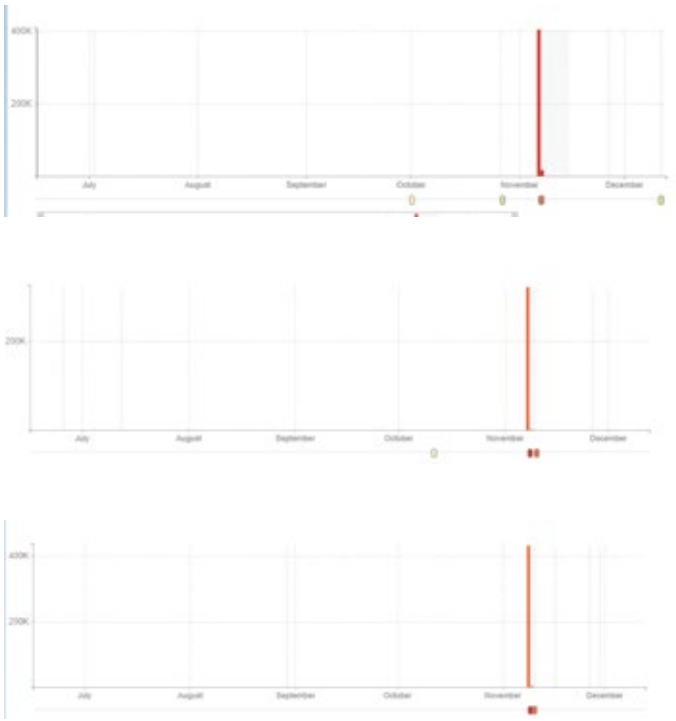
A trend that TNS has seen is a tactic of snowshoe spamming being employed by the bad actors. Snowshoe spamming is a strategy in which spam is propagated over several telephone numbers in low volume to avoid detection. The strategy of snowshoe spamming is like actual snowshoes that distribute the weight of an individual over a wide area to avoid sinking into the snow. Likewise, snowshoe spamming delivers its weight over a wide area of telephone numbers to remain clear of filters. The following two examples with similar phone numbers showed characteristics of snowshoe spamming.

## *Snowshoe spamming is an increasing tactic*



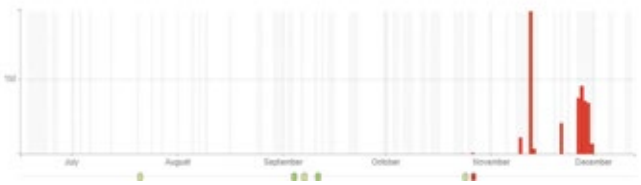

A similar trend is high-volume snowshoe spamming being employed by the bad actors. This type of spamming resembles neighbor spoofing where the bad actor will spoof a local number but will spread those calls in high volume over several numbers each day over several days, using deceptive call practices that are difficult to detect for OTT applications that are not integrated with the network like TNS Call Guardian. By the time the OTT application determines the number to be from a bad actor, the bad actor has moved on from that number.

Below is an example where a number placed over 400,000 calls from one number on a Tuesday, placed over 200,000 calls from a different number on Wednesday, placed 400,000 calls from a third number on a Thursday.



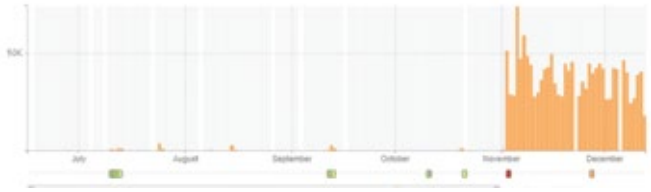
## *Neighbor spoofing and spreading the calls over multiple numbers is a tactic employed by bad actors*

A similar patterned occurred later in the month and all the numbers originated from the same area code and exchange.



The nature of this "scam" was a call from "Ann" who could offer lower health insurance costs, offering a hassle-free assessment if provided a social security number. The timing of the scam is not coincidental since the end of year is when open enrollment occurs, and health-care coverage needs to be renewed.

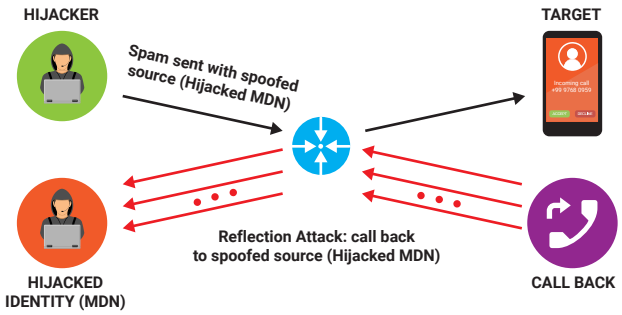
In addition, the toll-free number of the Health Insurance Marketplace was being used to place outbound calls near the end of the year. This agency doesn't make outbound calls to their subscribers.



## *Watch out for health insurance scams near the end of the year*

Another trend associated with snowshoe spamming that the TNS data scientists have picked up on is the hijacking of real wireless numbers. We estimate that 1 in 2,000 mobile directory numbers allocated to a cell phone subscriber was hijacked by spoofers in a 56 day-period.

The unsuspecting cell phone subscriber then receives a large number of reflective calls back from some of the numbers that the spoofer called. The outcome of these reflective calls is that the cell phone users discontinue use of nearly 1 in 5 hijacked mobile directory numbers.




*1 in 4,000 MDNs are hijacked every month*

In one extreme case, we saw a spoofer that used a legitimate mobile number to place over 20,000 calls.

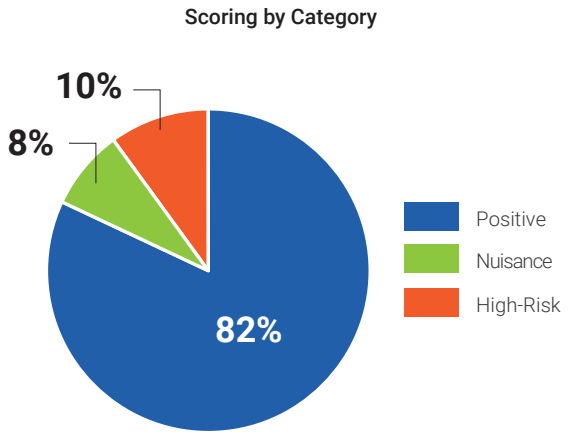
The wireless subscriber then received calls from nearly 6,000 numbers in a reflective callback on their mobile number.

## Canadian Results

In mid-December, the Commission in Canada mandated that universal network-level call blocking where the caller identification purports to originate from telephone numbers that do not conform to established numbering plans is to be implemented by Canadian carriers and other telecommunications service providers (TSPs) that provide voice telecommunications services within 12 months of the date of this decision. The mandate will not apply to those Canadian carriers and other TSPs providing voice telecommunications services that implement call filtering solutions within the time-frame prescribed for the implementation of universal network-level call blocking.

TNS Call Guardian product analyzes call events in Canada across carriers every day and bases robocall scoring and categorization on this data. Given this recent mandate, it is appropriate to include analysis on the Canadian market.

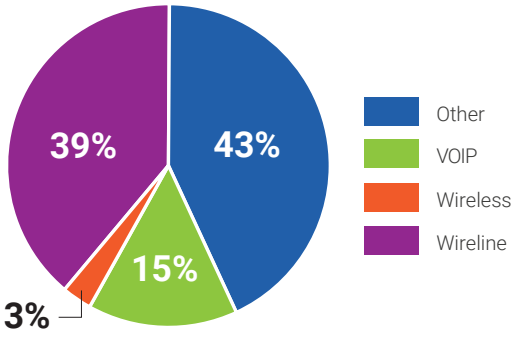
TNS found that roughly 20% of Canadian inter-carrier calls were scored negatively, less than in the United States, as summarized below:



Unlike the Unites States, wireline and other non-carrier assigned numbers lead in generating the majority of the nuisance calls in Canada.

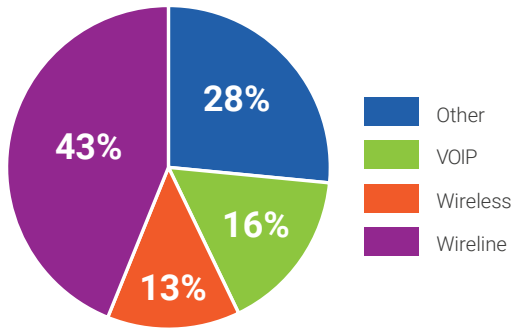
Again, the "other" category represents toll-free, malformed and invalid telephone numbers. A malformed telephone number is a telephone number that does not have 11 digits or that does not start with 1. An invalid telephone number, unlike a malformed telephone number, is well formed, but is not in a valid LERG block (NPA-NXX) and not in a valid toll-free area code.

**Distribution of Nuisance Calls**




However, most of the high-risk calls are from a wireline network and not surprisingly from a VoIP network.

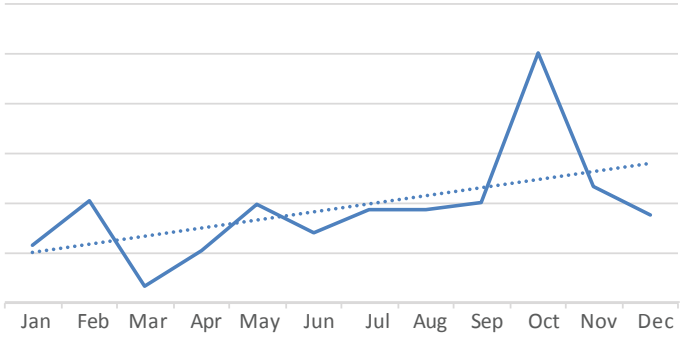
**Distribution of High-Risk Calls**



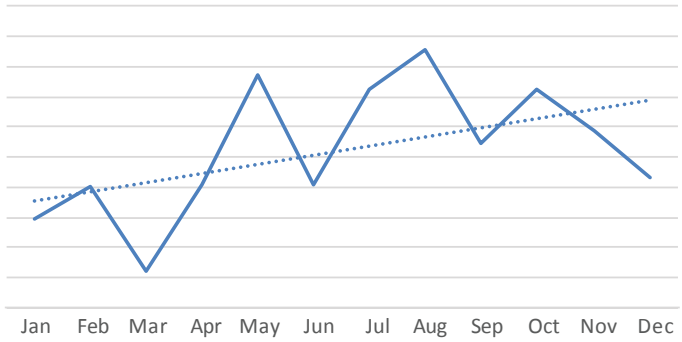

## *Originating negative traffic from Canada is growing at over 100%*

Nuisance and high-risk calling activity increased over 100% from the first quarter to the fourth quarter.

**Nuisance Calls by Month**




**High-Risk Calls by Month**



# Regulatory Updates

## Chairman Pai Demands Industry Adopt Protocols to End Illegal Spoofing

In early November, FCC Chairman Ajit Pai demanded that the phone industry adopt a robust call authentication system to combat illegal caller ID spoofing and launch that system no later than next year. Such a system is critical to protecting Americans from scam robocalls.

The FCC continues its exploration of methods to pursue bad actors, including blocking and tracebacks, and seeks the industry's help in its latest public notice to refresh the record on advanced methods to target and eliminate unlawful robocalls. Carriers and other industry experts involved in solving the robocall problem will be providing more detail about their approaches. Naturally, STIR/SHAKEN will play a significant role with respect to blocking and traceback efforts.

A robust call authentication framework is part of the Commission's multi-pronged effort to combat the scourge of spoofed robocalls. A robust call authentication framework would erode the ability of callers to illegally spoof their Caller ID, which scam artists use to trick Americans into answering their phones when they shouldn't. With a robust framework in place, consumers and law enforcement alike could more readily identify the source of illegal robocalls and reduce their impact.

## FCC Urges More in the Phone Industry to Join in Tracing Scam Robocalls

Also, in early November, the FCC sent letters to voice providers, calling on them to assist industry efforts to trace scam robocalls that originate on or pass through their networks.

The FCC receives more consumer complaints about unwanted calls—including scam calls that use spoofing to trick consumers—than any other subject. The agency uses these complaints and other resources to find bad actors and act.

## Commissioner Jessica Rosenworcel Calls on Industry to Provide Consumers with Free Robocall Blocking Tools

FCC Commissioner Jessica Rosenworcel is demanding action. In mid-December, she sent letters to major phone companies and is calling on carriers to offer free robocall blocking solutions to consumers across the country. Rosenworcel requested that each phone company provide a description of any tools to combat robocalls that they offer today, including a description of the costs charged, if any, to consumers.

## FCC Establishes Reassigned Phone Numbers Database to Help Reduce Unwanted Calls to Consumers

In mid-December, the FCC adopted new rules to establish a reassigned numbers database that will reduce the number of unwanted phone calls Americans receive.

Millions of phone numbers are reassigned each year. When a consumer gets a new phone number that was previously assigned to another consumer, businesses and other callers frequently do not learn of the reassignment right away and may inadvertently call the new consumer rather than the prior holder of the number. This results in the new consumer receiving unwanted calls and the prior number holder not receiving calls he or she expects, like notifications from a doctor's office, financial institution, or school.

The new rules establish a single, comprehensive database with information provided by phone companies that callers will be able to use to avoid calling reassigned numbers. Callers using the database will be able to find out if telephone numbers assigned to consumers who previously consented to their calls have subsequently been disconnected and made eligible for reassignment. Any such numbers can then be purged from their call lists, thereby decreasing the number of unwanted calls to consumers.

## Bipartisan TRACED Act Cracks Down on Illegal Robocall Scams

In mid-November, U.S. Senator John Thune (R-S.D.), chairman of the Senate Commerce, Science, and Transportation Committee, and Sen. Ed Markey (D-Mass.) a member of the committee and author of the Telephone Consumer Protection Act, announced a bill called the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. The TRACED Act gives regulators more time to find scammers, increases civil forfeiture penalties for those caught, promotes call authentication and blocking adoption, and brings relevant federal agencies and state attorneys general together to address impediments to criminal prosecution of robocallers who intentionally flout laws.

### The summary of the bill:

- Broadens the authority of the Federal Communications Commission (FCC) to levy civil penalties of up to $10,000 per call who intentionally flout telemarketing restrictions.
- Extends the window for the FCC to catch and take civil enforcement action against intentional violations to three years after a robocall is placed. Under current law the FCC has only one year to do so and the FCC has told the committee that "even a one-year longer statute of limitations for enforcement" would improve enforcement against willful violators.
- Brings together the Department of Justice, FCC, Federal Trade Commission (FTC), Department of Commerce, Department of State, Department of Homeland Security, the Consumer Financial Protection Bureau, and other relevant federal agencies as well as state attorneys general and other non-federal entities to identify and report to Congress on improving deterrence and criminal prosecution at the federal and state level of robocall scams.
- Requires providers of voice services to adopt call authentication technologies, enabling a telephone carrier to verify that incoming calls are legitimate before they reach consumers' phones.
- Directs the FCC to initiate a rulemaking to help protect subscribers from receiving unwanted calls or texts from callers using unauthenticated numbers.

## CRTC Compliance & Enforcement - Measures to Reduce Caller Identification Spoofing and to Determine the Origins of Nuisance Calls

In January, the Canadian Radio-television and Telecommunications Commission, indicated that it would initiate a proceeding to review the progress that is being made on caller identification (ID) authentication.

The Commission determined that authentication and verification of caller ID information for Internet Protocol (IP) voice calls should be implemented by Canadian telecommunications service providers (TSPs) by no later than March 31, 2019 to empower Canadians to better protect themselves against nuisance calls. TSPs are required to report on their progress. The Commission requested that the CRTC Interconnection Steering Committee (CISC) submit a consolidated industry progress report to the Commission every six months, beginning six months from the date of this decision.

## CRTC Compliance & Enforcement - Implementation of Universal Network-level Blocking of Calls with Blatantly Illegitimate Caller Identification

The CRTC followed up the January enforcement and in December mandated that universal network-level call blocking where the caller identification purports to originate from telephone numbers that do not conform to established numbering plans is to be implemented by Canadian carriers and other telecommunications service providers (TSPs) that provide voice telecommunications services within 12 months of the date of this decision. This mandate will not apply to those Canadian carriers and other TSPs providing voice telecommunications services that implement call filtering solutions within the time frame prescribed for the implementation of universal network-level call blocking.

*FCC & CRTC are expecting results from service providers*

# Industry Solutions to Combat Robocalling

## Hardware and Software

Solutions are available as both hardware and software products. Many products are limited to using only on a single medium, such as traditional copper landlines, or mobile phone contracts from a specific mobile phone operator.

Most over-the-top (OTT) software solutions are not integrated with a carrier network and rely on the use of honeypots, blacklists and whitelists, which are not entirely effective.

## Blacklists and Whitelists

In its simplest form, this method offers the ability to prevent further calls from phone numbers once they are known to be a source of robocalls. Many mobile apps can prevent robocalls with a user generated blacklist.

A major problem for the use of both blacklists and whitelists is the practice of caller ID spoofing which is prevalent because of the low barrier to entry in the VoIP services market.

## Landline Call Blockers

For landlines there are standalone call blockers which connect to the telephone. Various models work on blacklist and whitelist principles and are not entirely effective, like OTT software solutions. Several physical products have been developed for use with landlines. These are typically installed in homes and employ a hard coded or irregularly updated blacklist. Some models also have the ability to create a user-generated whitelist[10]. Newer devices for landlines can use cloud-based data to resolve the hard-coded blacklist issues and allow you to create your own whitelist/blacklist.

## Crowd-sourcing

A more sophisticated model uses crowd-sourcing to build a more comprehensive blacklist of robocall numbers.

Crowd-sourced feedback allows the analytics provider to layer in context. Supplementing the unstructured data provided by the machine learning methods, crowd-sourced data allows the analytics layer to provide information at a more granular level, such as whether a telephone number is being used as a claim to offer free cruises, or is a legitimate call from a bank with a fraud alert related to a credit card.

However, access to customer contacts can be problematic. OTT software solutions require users to provide access to their personal whitelist of genuine contacts, in exchange for access to the larger crowd-sourced database. In 2013, hackers gained access to one OTT provider's database of known genuine numbers, highlighting the danger of centralizing this information[11] [12].

## Do-Not-Originate

VoIP permits both legitimate and illegitimate caller name and number spoofing. Do-Not-Originate (DNO) involves the management of an outbound-calling blacklist consisting of the telephone numbers of financial institutions, government agencies, the 911 Do Not Call list, etc. used solely to receive inbound calls. This DNO list will be checked by VoIP gateways as they process outbound calls.

The goal is to block origination of calls from numbers that should never originate phone calls. These numbers belong to entities such as the IRS, often used in caller ID spoofing, usually with the intent to defraud. DNO could potentially allow the carrier to block any call that is using a non-allocated North American Numbering Plan NPA-NXX number, as well. On September 30, 2016, the FCC provided clarification that numbers added to the DNO list may be blocked by gateways[13].

While implementation of DNO is straightforward from a technical perspective, the challenges lie in the creation, maintenance, and security of the list server. Once established, future additions to the list will have to be authenticated. The authority for provisioning of this service will have to be established. Finally, similar telephone numbers will not be included in the database and may still be used for fraudulent purposes.

[10]https://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm
[11]https://blog.truecaller.com/2013/07/18/truecaller-statement/
[12]http://www.ehackingnews.com/2013/07/truecaller-database-hacked-by-syrian.html
[13] https://apps.fcc.gov/edocs_public/attachmatch/DA-16-1121A1.pdf

*STIR/SHAKEN will play a significant role with respect to blocking and traceback efforts*

## STIR/SHAKEN

While DNO is designed to prevent the origination of calls from telephone numbers that should not be making outbound calls, STIR/SHAKEN addresses identity authentication for calls traversing the SIP network to mitigate caller ID spoofing. STIR can be used both to validate origination in real-time and to perform a traceback, after a call is complete.

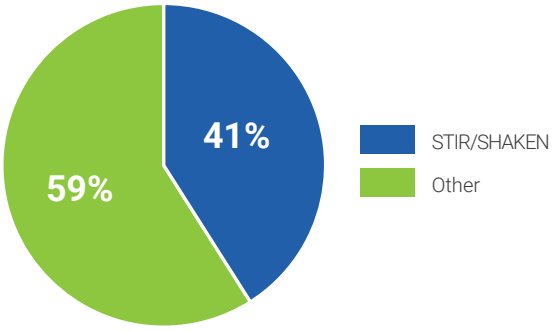
STIR/SHAKEN is more complex than DNO. STIR (Secure Telephone Identity Revisited) defines a signature to verify the calling number and specifies how it will be transported in SIP "on the wire". SHAKEN (Signature-based Handling of Asserted information using toKENs) is the framework document developed to provide an implementation profile for service providers implementing STIR.

STIR and SHAKEN use digital certificates, based on common public key cryptography techniques, to ensure the calling number of a telephone call is secure. In simple terms, each telephone service provider obtains their digital certificate from a certificate authority who is trusted by other telephone service providers. The certificate technology enables the called party to verify that the calling number is accurate and has not been spoofed.

STIR may only be used to authenticate and validate origination of the call for U.S. domestic calls and is applicable for SIP-to-SIP calls only. STIR is not applicable for TDM, nor will it work if the network path of the call traverses a legacy network, as opposed to an uninterrupted SIP-to-SIP call.

The tier 1 carriers that have indicated to the FCC that they will implement STIR/SHAKEN by 3Q19, account for less than 50% of the total traffic.

**Cross-Carrier Traffic Among Tier 1 Carriers**




STIR/SHAKEN can attest to the authentication of the calling party telephone number but is not able to address the question of intent. Bad actors will be able to make malicious calls from numbers that they have been assigned by a provider, and will be able to burn through those numbers, then move on to the use of new numbers to avoid detection.

STIR/SHAKEN is indisputably an essential foundational layer to combat spoofing. TNS also shares that it is crucial to understand its limitations and the ongoing need for the real-time analytics layer.

*STIR/SHAKEN needs to expand beyond the tier 1 providers for a call authentication framework to have a significant impact*

## Real-time Analytics

Once fully deployed, Do-Not-Originate and STIR/SHAKEN will provide crucial layers of protection. Among industry experts engaged in analysis of the issue, however, consensus is clear - a layered approach requiring access to an analytics server at the verification point is also required.

Today, it is possible to detect caller ID spoofing and other malicious and nuisance robocalling behavior based on real-time network data analytics. The analytics server uses advanced methods for blocking robocalls using real-time business intelligence techniques to address the constantly changing identities of robocalls. With access to a large enough data sample, it is possible to create algorithms which detect negative robocall activity without depending solely on crowd-sourced reporting.

Advanced machine learning methods for blocking robocalls using real-time artificial intelligence (AI) in combination with big data gleaned from the network effectively addressed the constantly changing identities of robocallers. This methodology makes it possible to create an algorithm which can detect call patterns without requiring crowd-sourced reporting.

Machine learning is a method used to devise complex models and algorithms that lend themselves to predictive analytics. The analytical models allow data scientists to produce reliable and repeatable decisions while also uncovering hidden insights through learning from historical relationships and trends in the data.

As an addition to this model, crowd-sourced feedback allows the analytics provider to layer in context. Supplementing the unstructured data provided by the machine learning methods, crowd-sourced data allows the analytics layer to provide information at a more granular level, such as whether a telephone number is being used to claim to offer free cruises or is a legitimate call from a bank with a fraud alert related to a credit card.

## Enterprise Response to Analytics

TNS has observed a varied response among enterprises to the mitigation techniques that the industry has employed. Among the good actors, although there has been discomfort with this new world in which their calls are being analyzed and characterized, there has been a general willingness to adapt methodologies to conform with the analytics tools' definitions of good behavior.

*Branded calling can restore trust to the voice calling experience*

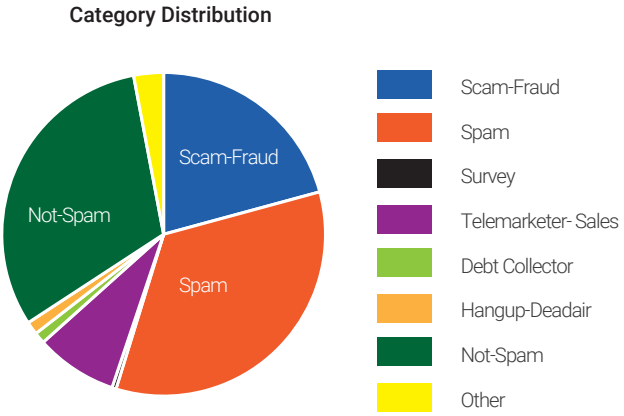
As a result, TNS has worked with partners and enterprise allies to develop tools such as Branded Calling, through which a logo and other business information may be displayed for legitimate calls. Further, TNS has developed a Reputation Insights product that provides call origination aggregators and enterprises with a view into their call centers' practices and allows them to understand how their numbers are being characterized, and when activity triggers negative reputational scores.

The registration of calling campaigns, for example, will yield positive results, as analytics engines better understand sudden spikes in calling traffic.

TNS has seen a dramatic increase in the number of telephone numbers that enterprises have registered either through the Reportarobocall website or the reputation monitoring service in just the last five months.

Specific to enterprises, one commonly observed trend is enterprises whose main outbound calling numbers are used for multiple purposes tend to get flagged by analytics engines and receive very mixed feedback from consumers. TNS recommends segmenting the use of toll-free numbers for various enterprise purposes. A number used for accounts receivable management, for example, should not be used for other purposes, as consumers will invariably provide negative feedback about the number which will impact other outreach efforts via the same number.

Below is an example showing the mixed customer feedback.




These and other initiatives can restore trust to the calling experience.

*Mixed customer feedback when using main calling number for multiple use cases*

# Conclusions and Recommendations

The FCC and CRTC continue exploration of methods to counter bad actors including blocking, adoption of protocols to prevent spoofing of numbers and tracebacks and has reached out to the service providers seeking the industry's help in their latest public notices to refresh the record on advanced methods to target and eliminate unlawful robocalls.

Carriers and other industry experts involved in solving the robocall problem will be providing more detail about their approaches. Naturally, STIR/SHAKEN will play a significant role with respect to blocking and traceback efforts.

*The robocall problem is more complex than it appears on its surface*

In addition, analytics providers will be explaining the complex role they play in overlaying context for robocalls that do not involve spoofing and providing the FCC with further insights regarding additional steps that can be taken to address this ongoing problem. The industry will be looking to the FCC for guidance and support as it seeks to further differentiate good calls from bad. Further, TNS will seek ways to support the FCC directives by onboarding data from vetted outbound callers and facilitating traceback efforts. It is encouraging to see this problem coming into greater relief as the industry works together to re-establish trust in calling.

The robocall problem is more complex than it appears on its surface. There are many solutions to combat robocalling, however, a layered approach will continue to be most effective. This layered approach includes the work being done to implement STIR/SHAKEN, the current analytics server role, and policy and structure around DNO.

The goal of this report is to share data and analysis that proves helpful to the industry and robocalling efforts of TNS partners. TNS will publish this report on a bi-annual basis to help the industry improve its security and detection today and adapt to what we will face in the future.

*A layered approach will be most effective in combating robocalls*

**To find out how TNS can help your organization combat Robocalls:**
**+ 1 703 453 8300 solutions@tnsi.com www.tnsi.com**